US006044471A

United States Patent [19]

Colvin

[11] Patent Number: 6,044,471

[45] Date of Patent: Mar. 28, 2000

[54] **METHOD AND APPARATUS FOR SECURING SOFTWARE TO REDUCE UNAUTHORIZED USE**

[75] Inventor: **David S. Colvin**, Commerce Township, Oakland County, Mich.

[73] Assignee: **Z4 Technologies, Inc.**, Commerce Township, Mich.

[21] Appl. No.: **09/090,620**

[22] Filed: **Jun. 4, 1998**

[51] **Int. Cl.**[7] **H04L 9/32**

[52] **U.S. Cl.** **713/202**; 709/229; 705/51

[58] **Field of Search** 714/202, 201, 714/200; 709/229; 380/3, 4, 23; 705/51, 52, 53, 55, 57, 59

[56] **References Cited**

U.S. PATENT DOCUMENTS

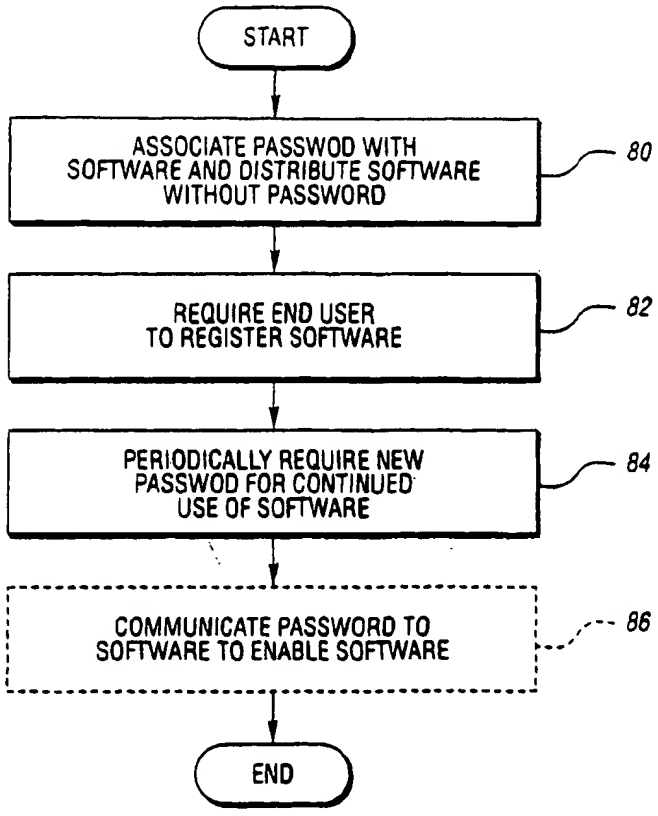
4,796,220	1/1989	Wolfe	380/4
5,182,770	1/1993	Medveczky et al. .	
5,287,408	2/1994	Samson .	
5,341,429	8/1994	Stringer et al.	705/52
5,509,070	4/1996	Schull .	
5,564,038	10/1996	Grantz et al. .	
5,579,479	11/1996	Plum	713/202
5,652,793	7/1997	Priem et al. .	
5,842,124	11/1998	Kenagy et al.	455/411

Primary Examiner—Robert W. Beausoliel, Jr.
Assistant Examiner—Christopher A. Revak
Attorney, Agent, or Firm—Brooks & Kushman P.C.

[57] **ABSTRACT**

A method and apparatus for securing software to reduce unauthorized use include associating a password or series of passwords with each copy of group of authorized software and requiring entry of a first password obtained from the developer or authorized representative of the software after exchanging registration information. The method and apparatus may also subsequently require entry of a second password from the series associated with the software to continue using the software. A password or authorization code series may be associated with each authorized copy or with a group of copies such as those distributed to a particular organization or site. Preferably, subsequent passwords or authorization codes are obtained from an authorized software developer, manufacturer, or distributor which gathers current information from the user to monitor compliance with licensing restrictions. The number and frequency of required password updates may be regular or irregular depending upon the application, user, or software manufacturer. A code which disables the software may be communicated if the manufacturer determines that the user is an unauthorized user.

45 Claims, 6 Drawing Sheets



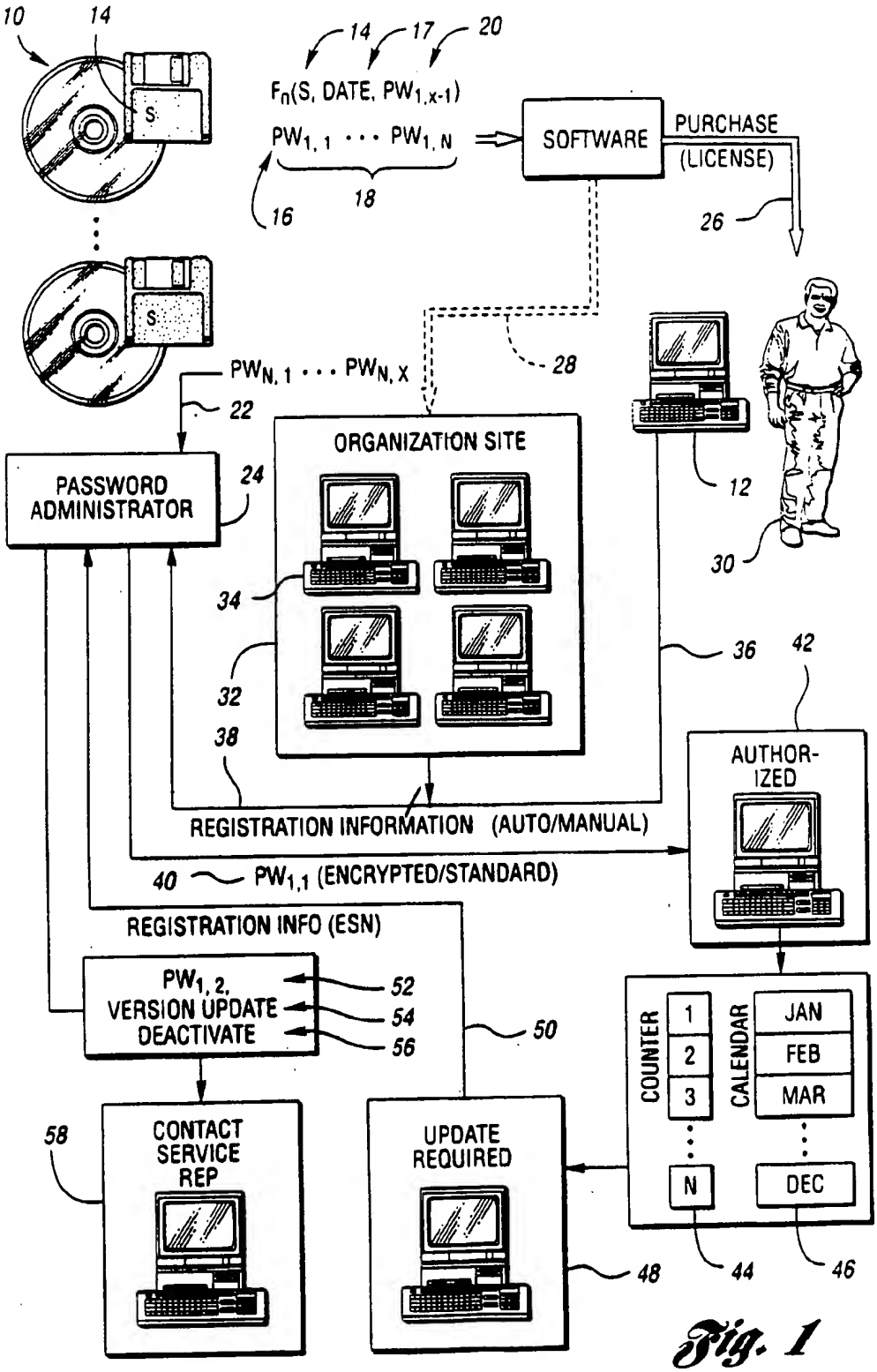

10
14
S
S
14
17
20
F_n(S, DATE, $PW_{1,x-1}$)
$PW_{1,1}$ ··· $PW_{1,N}$
16
18
SOFTWARE
PURCHASE
(LICENSE)
26
28
$PW_{N,1}$ ··· $PW_{N,X}$
22
PASSWORD ADMINISTRATOR
24
ORGANIZATION SITE
34
32
38
12
30
36
42
AUTHOR-IZED
REGISTRATION INFORMATION (AUTO/MANUAL)
40
$PW_{1,1}$ (ENCRYPTED/STANDARD)
REGISTRATION INFO (ESN)
$PW_{1,2}$,
VERSION UPDATE
DEACTIVATE
52
54
56
50
COUNTER
1
2
3
N
CALENDAR
JAN
FEB
MAR
DEC
58
CONTACT SERVICE REP
UPDATE REQUIRED
48
44
46

Fig. 1

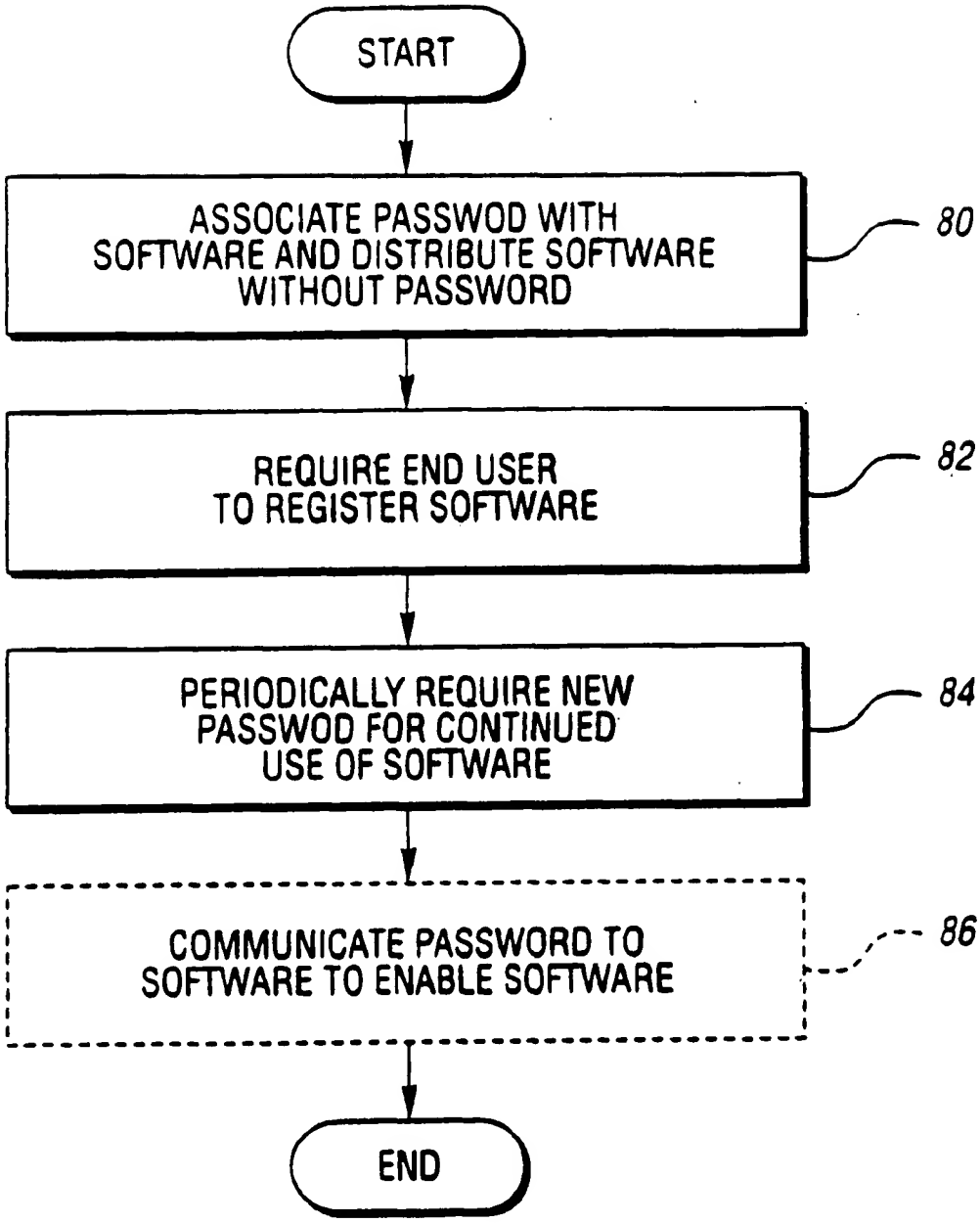

START
ASSOCIATE PASSWOD WITH SOFTWARE AND DISTRIBUTE SOFTWARE WITHOUT PASSWORD
80
REQUIRE END USER TO REGISTER SOFTWARE
82
PERIODICALLY REQUIRE NEW PASSWOD FOR CONTINUED USE OF SOFTWARE
84
COMMUNICATE PASSWORD TO SOFTWARE TO ENABLE SOFTWARE
86
END

Fig. 2

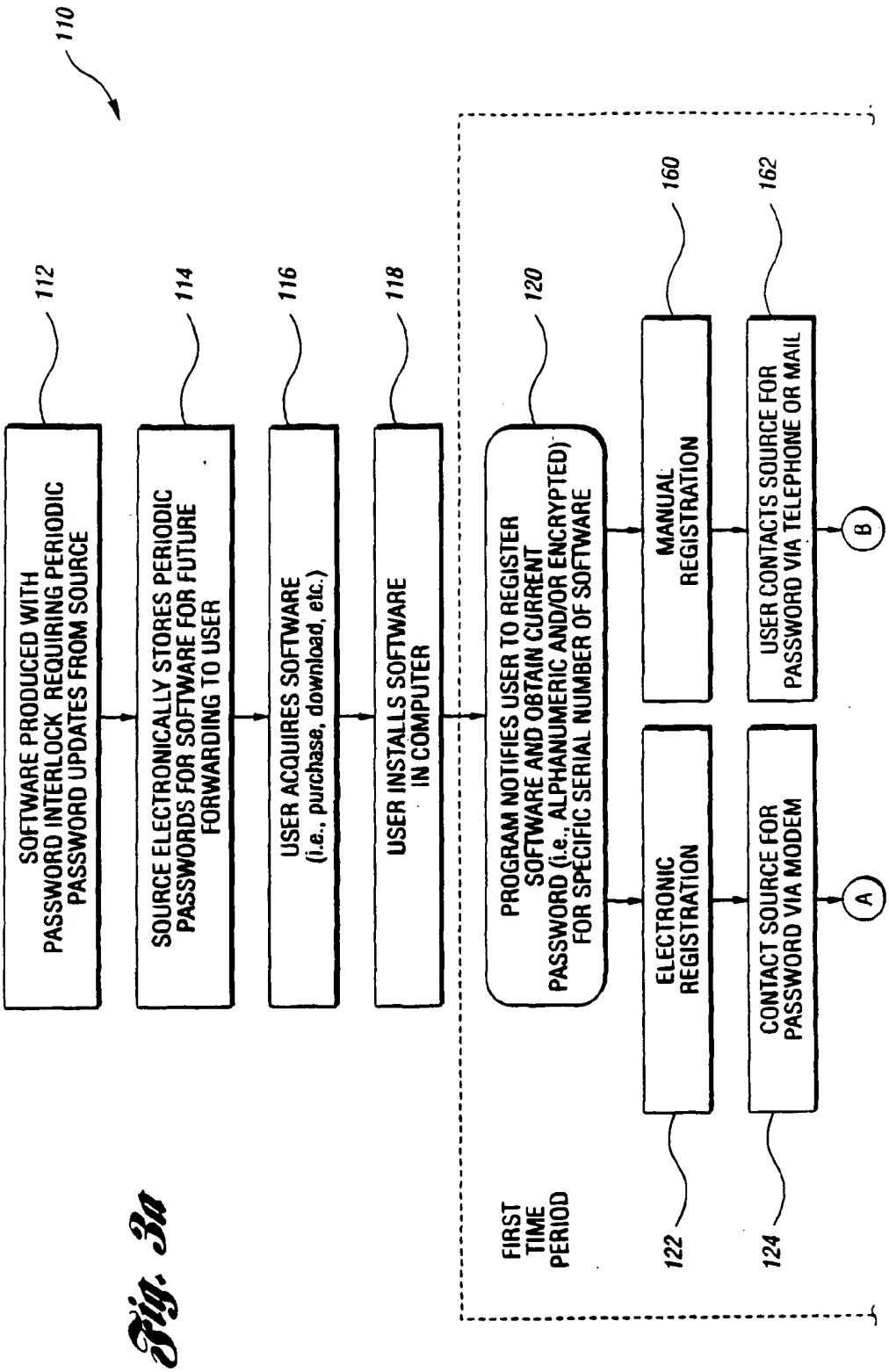

110
112
SOFTWARE PRODUCED WITH PASSWORD INTERLOCK REQUIRING PERIODIC PASSWORD UPDATES FROM SOURCE
114
SOURCE ELECTRONICALLY STORES PERIODIC PASSWORDS FOR SOFTWARE FOR FUTURE FORWARDING TO USER
116
USER ACQUIRES SOFTWARE (i.e., purchase, download, etc.)
118
USER INSTALLS SOFTWARE IN COMPUTER
120
PROGRAM NOTIFIES USER TO REGISTER SOFTWARE AND OBTAIN CURRENT PASSWORD (i.e., ALPHANUMERIC AND/OR ENCRYPTED) FOR SPECIFIC SERIAL NUMBER OF SOFTWARE
160
MANUAL REGISTRATION
162
USER CONTACTS SOURCE FOR PASSWORD VIA TELEPHONE OR MAIL
B
ELECTRONIC REGISTRATION
CONTACT SOURCE FOR PASSWORD VIA MODEM
A
FIRST TIME PERIOD
122
124

Fig. 3a

Fig. 3b

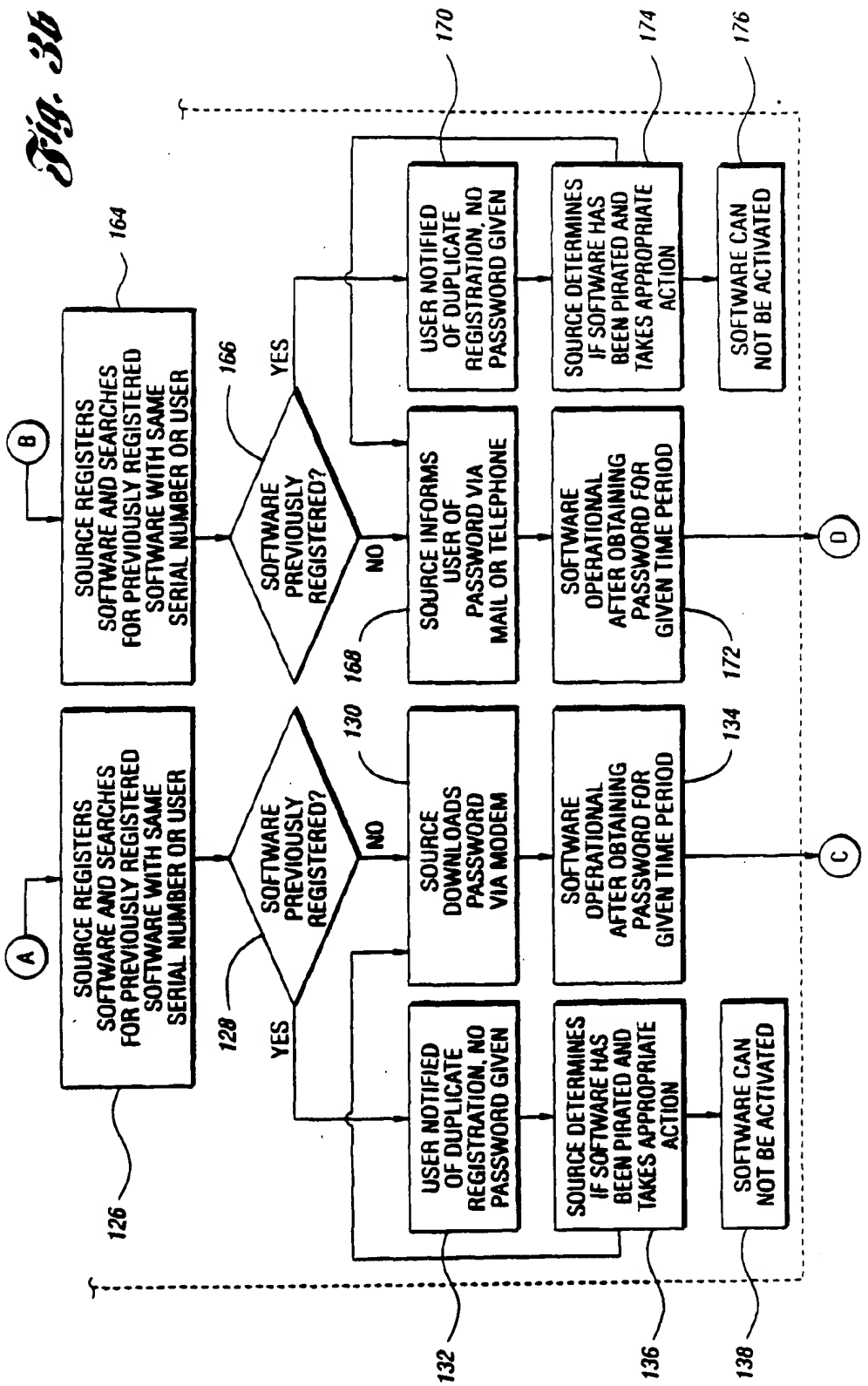
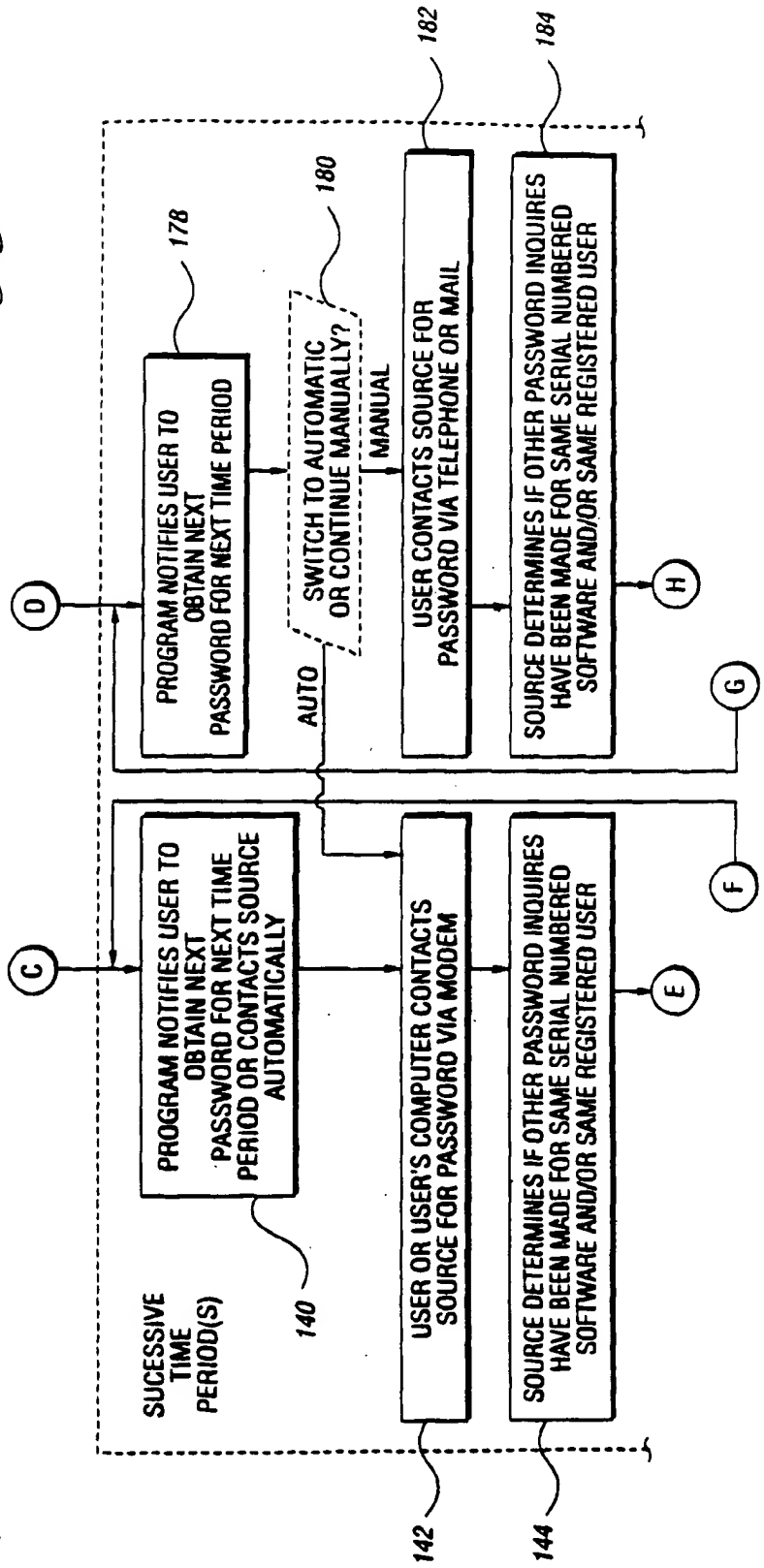

A
B
C
D
SOURCE REGISTERS SOFTWARE AND SEARCHES FOR PREVIOUSLY REGISTERED SOFTWARE WITH SAME SERIAL NUMBER OR USER
126
SOFTWARE PREVIOUSLY REGISTERED?
128
YES
NO
SOURCE DOWNLOADS PASSWORD VIA MODEM
130
SOFTWARE OPERATIONAL AFTER OBTAINING PASSWORD FOR GIVEN TIME PERIOD
134
USER NOTIFIED OF DUPLICATE REGISTRATION, NO PASSWORD GIVEN
132
SOURCE DETERMINES IF SOFTWARE HAS BEEN PIRATED AND TAKES APPROPRIATE ACTION
136
SOFTWARE CAN NOT BE ACTIVATED
138
SOURCE REGISTERS SOFTWARE AND SEARCHES FOR PREVIOUSLY REGISTERED SOFTWARE WITH SAME SERIAL NUMBER OR USER
164
SOFTWARE PREVIOUSLY REGISTERED?
166
YES
NO
SOURCE INFORMS USER OF PASSWORD VIA MAIL OR TELEPHONE
168
SOFTWARE OPERATIONAL AFTER OBTAINING PASSWORD FOR GIVEN TIME PERIOD
172
USER NOTIFIED OF DUPLICATE REGISTRATION, NO PASSWORD GIVEN
170
SOURCE DETERMINES IF SOFTWARE HAS BEEN PIRATED AND TAKES APPROPRIATE ACTION
174
SOFTWARE CAN NOT BE ACTIVATED
176

Fig. 3c


SUCESSIVE TIME PERIOD(S)
PROGRAM NOTIFIES USER TO OBTAIN NEXT PASSWORD FOR NEXT TIME PERIOD OR CONTACTS SOURCE AUTOMATICALLY
140
USER OR USER'S COMPUTER CONTACTS SOURCE FOR PASSWORD VIA MODEM
142
SOURCE DETERMINES IF OTHER PASSWORD INQUIRES HAVE BEEN MADE FOR SAME SERIAL NUMBERED SOFTWARE AND/OR SAME REGISTERED USER
144
C
E
F
PROGRAM NOTIFIES USER TO OBTAIN NEXT PASSWORD FOR NEXT TIME PERIOD
178
SWITCH TO AUTOMATIC OR CONTINUE MANUALLY?
180
AUTO
MANUAL
USER CONTACTS SOURCE FOR PASSWORD VIA TELEPHONE OR MAIL
182
SOURCE DETERMINES IF OTHER PASSWORD INQUIRES HAVE BEEN MADE FOR SAME SERIAL NUMBERED SOFTWARE AND/OR SAME REGISTERED USER
184
D
G
H

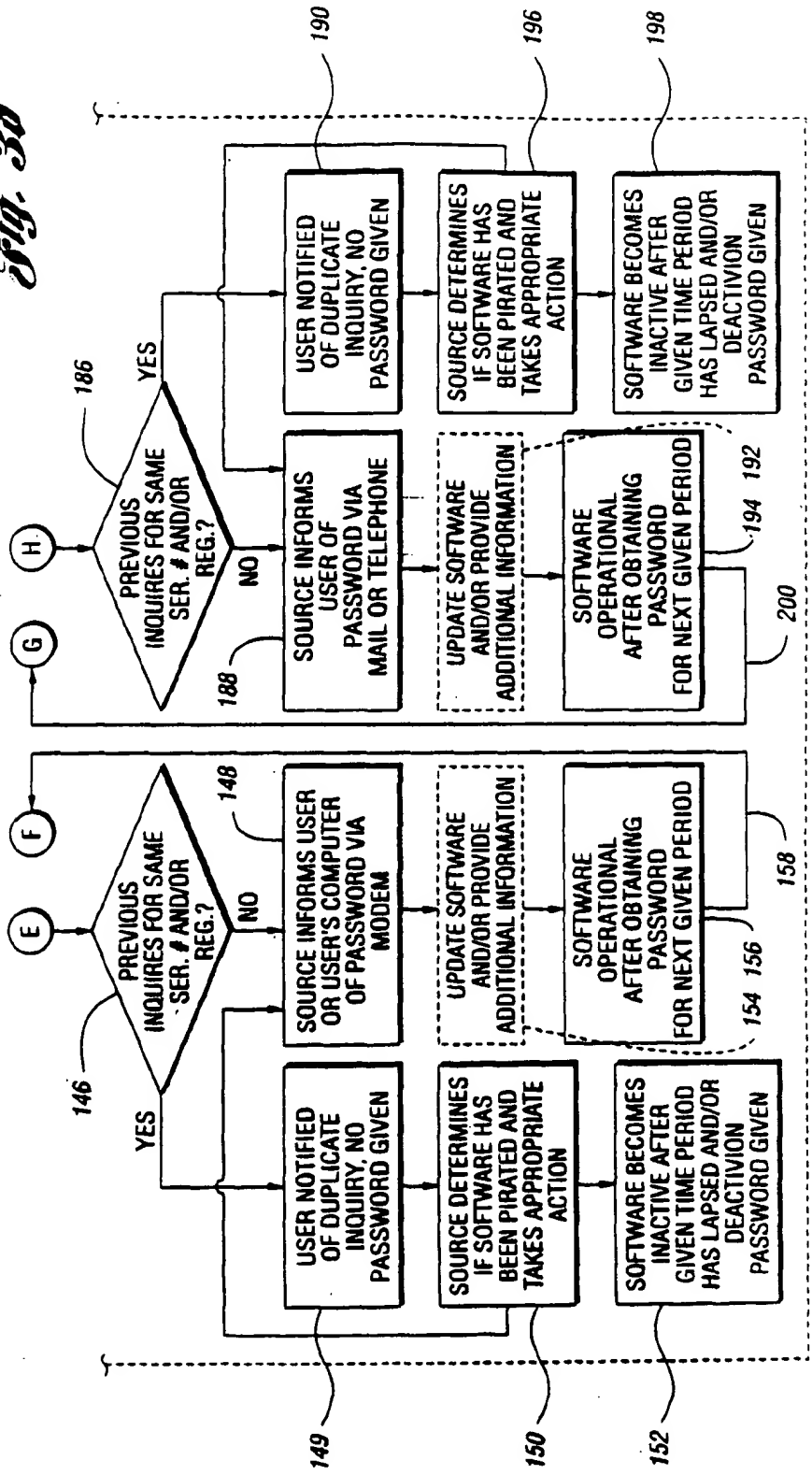


Fig. 3b
E
F
G
H
PREVIOUS INQUIRES FOR SAME SER. # AND/OR REG.?
146
YES
NO
148
SOURCE INFORMS USER OR USER'S COMPUTER OF PASSWORD VIA MODEM
UPDATE SOFTWARE AND/OR PROVIDE ADDITIONAL INFORMATION
SOFTWARE OPERATIONAL AFTER OBTAINING PASSWORD FOR NEXT GIVEN PERIOD
154
156
158
USER NOTIFIED OF DUPLICATE INQUIRY, NO PASSWORD GIVEN
149
SOURCE DETERMINES IF SOFTWARE HAS BEEN PIRATED AND TAKES APPROPRIATE ACTION
150
SOFTWARE BECOMES INACTIVE AFTER GIVEN TIME PERIOD HAS LAPSED AND/OR DEACTIVION PASSWORD GIVEN
152
PREVIOUS INQUIRES FOR SAME SER. # AND/OR REG.?
186
YES
NO
188
SOURCE INFORMS USER OF PASSWORD VIA MAIL OR TELEPHONE
UPDATE SOFTWARE AND/OR PROVIDE ADDITIONAL INFORMATION
SOFTWARE OPERATIONAL AFTER OBTAINING PASSWORD FOR NEXT GIVEN PERIOD
192
194
200
USER NOTIFIED OF DUPLICATE INQUIRY, NO PASSWORD GIVEN
190
SOURCE DETERMINES IF SOFTWARE HAS BEEN PIRATED AND TAKES APPROPRIATE ACTION
196
SOFTWARE BECOMES INACTIVE AFTER GIVEN TIME PERIOD HAS LAPSED AND/OR DEACTIVION PASSWORD GIVEN
198

METHOD AND APPARATUS FOR SECURING SOFTWARE TO REDUCE UNAUTHORIZED USE

TECHNICAL FIELD

The present invention relates to apparatus and methods for reducing unauthorized use of software.

BACKGROUND ART

Software developers are often victims of illicit copying and unauthorized use of their software in violation of contractual obligations imposed by licensing agreements and subject to civil and criminal penalties under various domestic and foreign laws. Unauthorized entities range from a relatively small percentage of the total users to an overwhelming majority of illegal users. Such unauthorized use not only amounts to theft of the developers' intellectual property, but also reduces the number of programs sold and therefore the associated profitability of the developer. This may ultimately diminish the creative effort expended by the software developers due to the reduced financial incentive. The advent of the internet has contributed to the proliferation of pirated software, known as "warez", which is easily located and readily downloaded.

Various strategies have been employed to make unauthorized duplication and use of software more difficult. One such approach is to provide a hardware "key" which is typically installed in the parallel port of the computer to provide a software interlock. If the key is not in place, the software will not execute. This method is relatively expensive for the developer and cumbersome for the authorized user while remaining vulnerable to theft by duplication of the hardware key.

Another approach requires the user to enter a serial number or customer identification number during installation of the software. Missing or invalid registration information prevents installation of the software. This approach is easily defeated by transferring the serial number or customer identification number to one or more unauthorized users.

Yet another approach requires registering the software with the manufacturer or distributor to obtain an operational code or password necessary for installation of the software. Again, once the operational code or password is obtained, it may be perpetually transferred along with pirated copies to numerous unauthorized users.

Various copy protection strategies have been employed to reduce the number of unauthorized copies available. This approach is generally disfavored by users who may have a legitimate need to make backup or archival copies or transfer a copy to a new computer or hard drive.

While prior art strategies have enjoyed various levels of success in reducing unauthorized use of software, they often impose a significant burden on the authorized users or are easily defeated by unauthorized users. As such, software developers need an apparatus and/or method for reducing unauthorized use of software which does not burden the authorized users to dissuade them from purchasing and using the protected software.

SUMMARY OF THE INVENTION

Thus, one object of the present invention is to provide an apparatus and method for improving software security throughout the lifetime of the software.

Another object of the present invention is to provide an apparatus and method for monitoring the number of users of a software product, both authorized and unauthorized.

Yet another object of the present invention is to provide an apparatus and method for the software manufacturer to maintain contact with the user over an extended period of time.

A further object of the present invention is to provide a method and apparatus for reducing unauthorized use of software which facilitate periodic software updates and forwarding of information, when and if desired.

A still further object of the present invention is to identify those entities responsible for unauthorized copying or use of software so that appropriate action may be taken, such as disabling the software, requesting payment from the user, or seeking civil or criminal penalties.

Another object of the present invention is to provide a method and apparatus for reducing unauthorized software use which deactivates unauthorized copies when an unauthorized user attempts to obtain a password.

In carrying out the above objects and other objects, features, and advantages of the present invention, a method for securing software includes associating a series of passwords or authorization codes with each copy or group of authorized software, requiring entry of a first password from the series associated with the software upon first use of the software, and subsequently requiring entry of a second password from the series associated with the software to continue using the software. A password or authorization code series may be associated with each authorized copy or with a group of copies such as those distributed to a particular organization or site. Preferably, subsequent passwords or authorization codes are obtained from an authorized software developer, manufacturer, or distributor which gathers current information from the user to monitor compliance with licensing restrictions. The number and frequency of required password updates may be regular or irregular depending upon the application, user, or software manufacturer.

The present invention contemplates, but does not require, more frequent password updates for more complex software because it is generally more costly to develop (and therefore more valuable to users) whereas less costly software would require fewer password updates to reduce administrative costs associated with password maintenance.

Password or authorization code updates may be obtained automatically or manually. Automatic updates are accomplished using electronic communication between the manufacturer's computer (or an authorized representative) and the user's computer. Updates may be performed by a direct modem connection, via email, a web browser, or the like. The particular time an nature of updates and the user interface utilized to implement the updates may vary by manufacturer or product. Manual updates are performed by advance or periodic notifications generated by the software to alert the user that password updates are required or will be required in the near future. The user may then contact the manufacturer for the specific password update via telephone, mail, email, or the like. Password advisories normally occur prior to the periodic termination of the operating period which may be measured by program starts, elapsed running time, calendar period, etc. Password updates may be in the form of alphanumeric and/or encrypted passwords or of any other conventional type.

Preferably, the user must provide registration information prior to receiving the original or updated password or authorization code. Registration information may be entered by the user or automatically acquired (and transmitted for automatic updates) by the software. Registration informa-

tion may include a serial number, registration number, TCP/IP address, user name, telephone number, computer specific information, etc. This information may be encoded and/or encrypted to make it less susceptible to tampering by unauthorized users. The registration information is preferably monitored and compared to previously captured information to control the number of authorized copies of software and/or identify unauthorized users. If unauthorized use is suspected, a password or authorization code may be provided which subsequently disables the software, either immediately or after some period of time so that an authorized user is provided an opportunity to rectify the information which caused deactivation.

A number of advantages result from various implementations of the present invention. For example, the present invention reduces unauthorized use of software without imposing a significant burden on authorized users. The present invention controls the number of copies of authorized software by monitoring registration information and deactivation of suspected pirated copies. Requiring authorized users to periodically update a password or authorization code provided by a password administrator improves accuracy of contact information for marketing related products and distribution of product updates. The present invention also provides a variable level of software security which can be tailored to the particular application depending upon the value of the application to potential software pirates.

The above advantages and other advantages, objects, and features of the present invention will be readily apparent from the following detailed description of the best mode for carrying out the invention when taken in connection with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating various features of a method and apparatus for securing software according to the present invention;

FIG. **2** is a flow diagram illustrating generally a method for securing software according to the present invention; and

FIGS **3***a* through **3***d* is a more detailed flow diagram illustrating representative embodiments of a method and apparatus for securing software according to the present invention.

BEST MODE(S) FOR CARRYING OUT THE INVENTION

Referring now to FIG. 1, a block diagram illustrating various features of a method and apparatus for securing software according to the present invention is shown. Manufacturers or developers create application programs or software which is stored in the form of data representing program instructions executable by a computer on computer readable media **10**. Computer readable media **10** may include any medium capable of storing such instructions which is directly or indirectly readable by a computer, such as computer **12**. Computer readable media may include floppy disks, hard drives, CD-ROMs, floptical disks, magnetic tape, and the like. Each copy or group of copies of the software may have an associated serial number, indicated generally by reference numeral **14**, and an associated password **16** which may be one of a series of associated passwords **18** as explained in greater detail below. Each password **16** may be an alphanumeric character string which may be encoded or encrypted or a binary or hexadecimal machine readable string to resist tampering by unauthorized users. Passwords **16** within series **18** may be randomly assigned or may be generated using a suitable algorithm, many of which are known in the art. Likewise, passwords **16** may be based on serial number **14**, a current data or version data **17**, and/or a previous password **20** from the series of passwords.

After the password or passwords are created and associated with one or more serial numbers or copies of the software, they may be transferred to an authorized representative of the software, as represented by arrow **22**, such as a password administrator **24**. Of course, the original manufacturer or developer of the software may also function as password administrator **24**. The software may be distributed by purchase or more commonly it is licensed as represented by arrows **26** and **28** to individuals **30** and groups **32**, respectively. Preferably, the software is distributed to the end users without its associated password **16** which must be obtained from password administrator **24**. Alternatively, computer readable media **10** may be distributed with the first password **16** of a series of passwords **18**. Each authorized user preferably has software with a unique identifier, such as a serial number, whether the authorized user is an individual, such as user **30**, or a group or region, indicated generally by reference numeral **32**. However, the same password or series of passwords may be associated with a number of serial numbers to reduce the administrative burden for password administrator **24**. For example, each end user **34** associated with organization or site **32** may have the same password or series of passwords. Preferably, not more than one password is distributed with each authorized copy so that the end users will need to contact password administrator **24** to obtain additional passwords for continued use of the software as explained in greater detail below.

During the initial use or installation of the software on computers **12,34**, a password or authorization code will be required by the software to function properly. The end user must contact the authorized representative for the software, such as password administrator **24**, to obtain the appropriate authorization code or password as indicated generally by arrows **36**. Password administrator **24** obtains registration information **38** from the end user and provides an appropriate password or authorization code to the software as indicated by reference numeral **40**. Communication of registration information and the authorization code may be accomplished either manually or automatically depending upon the particular application and configuration of the software. Manual communication may be by email, regular mail, telephone, automated voice response system, web browser, direct modem transfer, or the like but requires a varying level of intervention by the end user depending upon the particular type of communication. Automatic communication may use similar methods or means to communicate the information but is performed without user intervention, although the user may be advised or notified that the process is occurring or has occurred.

Registration information **38** may include traditional contact information, such as name, address, email, phone, etc. but preferably includes information which can be obtained without intervention by the end user to improve its veracity. Such information may include identification of a TCP/IP address, originating telephone number, or computer-specific information associated with the end user. Computer-specific information may include an electronic serial number (ESN) which uniquely characterizes the hardware configuration of the computer based on information stored in the computer's non-volatile CMOS, registry, motherboard serial number, or the like. Password administrator **24** preferably stores the registration information to be used for various purposes

according to the present invention to reduce unauthorized use of software. For example, password administrator **24** may use the registration information to monitor compliance with licensing terms by determining whether a particular serial number has been installed on more than one computer or by more than one end user. Administrator **24** may compare the registration information with previously received registration information to determine whether to issue an authorization code or password, or to provide a code which disables further operation of the software. The registration information may also be used to contact the end users for marketing new products or versions, or providing software updates.

The password or authorization code is communicated to the software as represented by reference numeral **40**. Depending upon the particular implementation, the password may be provided to the end user who manually enters the information into the computer **42** to begin or continue using the software. The password or authorization code may be encoded as an alphanumeric string using various numbers and letters which represent meaningful information to the administrator but appear to be randomly generated to the end user. Alternatively, an encryption algorithm may be used to transmit the information. Preferably, the password authorizes the software to execute on computer **42** for a first predetermined period as represented by counter **44** or calendar **46**. The predetermined period may vary based on the particular authorized user, the cost of the software, the number of estimated unauthorized copies etc. For example, it is anticipated that more expensive software would provide a shorter period of authorization to provide a higher level of security. The higher revenue generated by the software offsets any increased administrative expense of password administrator **24** due to the increased frequency of updates required.

As indicated by counter **44** and calendar **46**, the authorized period of use may be measured either in calendar days (months, years etc.) or in execution hours, number or accesses, or the like. Once the authorized code as indicated by reference numeral **48**. This may be accomplished automatically and transparently to the end user by electronically contacting password administrator **24** and exchanging current registration information **50**. Administrator **24** may compare the current registration information **50** with previously received registration information to determine if at least a portion of the information matches for that particular serial number or group of serial numbers. This comparison may be used to determine whether the end user is an authorized user or an unauthorized user.

The information provided to the software by administrator **24** may depend upon whether the user is determined to be authorized or unauthorized. For example, if the user is determined to be an authorized user, a subsequent password **52** from the series of passwords associated with the software serial number or group may be communicated which authorizes the software for an additional operation period. As the software becomes less valuable, such as when new versions are released, the authorization period may increase and preferably eventually allows indefinite use of the software. Of course, an exceedingly long period (10 years for example) may be essentially equivalent to an indefinite period of operation. In addition to a subsequent password, an updated version **54** of the software may be transferred or offered to the end user. If the user is determined to be an unauthorized user, an appropriate message may be transmitted to alert the user to a discrepancy in the registration information, and the operational password may be withheld. Alternatively or in addition, a code **56** which deactivates the software may be communicated. As another alternative, a shortened authorization period may be provided along with a password and a message which indicates the end user must contact administrator **24** or another customer service representative to verify the user's status as represented by reference numeral **58**. In the event the user is determined to be unauthorized, password administrator **24** may decline to download a password at which time the software may automatically become inoperative after the current operational period has lapsed.

Referring now to FIG. **2**, a flow diagram generally illustrating a method for securing software according to the present invention is shown. A password or series of passwords is associated with a particular copy or group of copies of software prior to distribution (without the password or with only one of a series of passwords) as represented by block **80**. A series of passwords may be associated with the software using an appropriate password generation algorithm with parameters which vary based on the particular copy. For example, a algorithm or mathematical equation or formula may be used to generate passwords with one or more of the parameters of the equation corresponding to letters or characters in the serial number of the software.

For applications which have only a single password for each copy or group of copies, the password may not be distributed with the software so the end user must contact the developer or authorized representative as represented by block **82**. For applications with two or more passwords, an initial password may be provided or the software may operate without a password for a first period to provide ample opportunity for the end user to acquire the initial/subsequent password. Registration information may be required as a precondition to providing a valid authorization code or password. This allows the developer or authorized representative to monitor compliance with licensing terms and/or take appropriate action for unauthorized users.

The password or authorization code is communicated to the software as represented by block **84** to make the software operational on the end user's computer. This may be performed automatically, without user intervention, or manually when initiated by the user using various communication channels, such as regular mail, email, web browser, direct modem connection, etc. The method may optionally require periodic updates at regular, irregular, or random intervals based on elapsed running time, calendar time, or the like, as represented by block **86**. The software may prompt the user when the end of the authorization period is approaching to provide an opportunity to obtain a subsequent authorization code for continued use of the software.

Referring now to FIG. **3***a*, a more detailed flow diagram illustrating a method and/or apparatus for securing software according to the present invention is shown. The software manufacturer or developer (source) produces software which requires initial and/or periodic password updates to become or to remain operational as depicted in box **112**. Software may be associated with individual end users, a regional (geographic) or other group of users, or users associated with a particular organization or site. Providing passwords or authorization codes for groups rather than each individual significantly reduces the number of passwords required and the corresponding administrative overhead including electronic storage and transmission requirements.

Following production by the software manufacturer, the source electronically stores the password information for future transmission to the user as shown in box **114**. The

password information may be the actual passwords or information used to generate subsequent passwords based on the individual copy or group of copies of the software. The embodiment depicted in FIG. 3*a* is intended to interlock specific pieces or groups of software with corresponding passwords or authorization codes.

Once the software is acquired by the user **116**, the user installs (partially or fully) the software in his computer or computer network **118**. Following installation of the software, the user is prompted to register the software and obtain the necessary operational password which may be an alphanumeric string which is encoded or encrypted, or a binary (machine readable) code. The user is allowed to choose between automatic or manual registration **120**. As shown in FIG. 3*b*, if automatic registration is selected **122**, the program automatically contacts the source via a modem or other connection to obtain the operational password following registration **124**.

Once contacted, the source searches for previous registration of the software with the registration number or user identification **126**, if the software has not been previously registered **128**, the source transmits the necessary password **130** wherein the software becomes operational **134**. If registration information has been previously entered and does not match the current registration information, the source notifies the user of a previous registration of the same software **132** and thereafter takes appropriate action **136**. Such action can either include denying the necessary operational password **138**, continuing the password download if the source desires **130** or other appropriate action or actions.

Following the initial registration of the software and downloading of the first operational password, the software remains operational for a given interval which may be an operation period or time period (random, regular, or irregular). Once the first interval expires, the program notifies the user of the necessity to obtain the next operating password **140** as shown in FIG. 3*c*. The user's computer contacts the source via modem **142** and the source determines if previous inquires have been made for the same user **144** based on the registration information. These step(s) may be fully automated, thereby eliminating the need for user intervention or notifying the user.

As shown in FIG. 3*d*, the source either transmits the password **148** or notifies the user of a duplicate inquiry **149**. If a duplicate inquiry has been made, the source either declines to download **150** the password so that the software becomes non-operational **152** after the current operational period elapses or the source transmits the password **148** if desired. During any of the contact periods between the source and the user, the source may elect to download software updates or additional information **154**. Following the downloading or the necessary operational password, the software becomes or remains operational **156**. This sequence is selectively repeated **158** as determined by the authorization interval selected by the source and communicated to the software.

As shown in FIG. 3*a*, the user may have the option of manual registration **160** and password input as opposed to automatic registration. Alternatively, the source may require manual registration to verify the accuracy of at least some of the registration information since it will be used to send the authorization code or password to the user. If the user provides inaccurate information, the password will not be transmitted and the software will not be operational. After initial registration, optionally the user may elect to convert to automatic electronic contact at any time. Where manual registration is selected **160** (or required), the user contacts the source via telephone, mail, email, internet, or the like to obtain the operational password following registration **152**.

Once contacted, the source searches for previous registration of the software with the same serial number, registration number or user identification **164** as shown in FIG. 3*b*. If the software has not been previously registered **166**, the source transmits the necessary password **168** wherein the software becomes operational **172**. If a duplicate registration occurs, the source notifies the user of a previous registration of the same software **170** and thereafter takes appropriate action **174**. Such action can either include not providing the necessary operational password **176** or continuing the password transmission if the source desires **168**.

Following the initial registration of the software and transmission of the first operational password, the software remains operational for a given operation interval after which the software notifies the user of the necessity to obtain the next operating password **178** as shown in FIG. 3*c*. The user contacts the source via telephone or by mail **182** and the source determines if previous inquiries have been made for the same user **184**. The user may elect to convert to automatic electronic registration during this period **180**, however, this step is operational.

In FIG. 3*d*, the source either transmits the password **188** or notifies the user of a duplicate inquiry **190**. If a duplicate inquiry has been made, the source either declines to download the password **196** (after which the software becomes non-operational **198**) or the source transmits the password **188** if desired. During any of the contact periods between the source and the user, the source may elect to transmit software updates or additional information **192**. Following the downloading or the necessary operational password the software becomes or remains operational **194**. The sequence for successive operation intervals may then be repeated at the source's discretion **200**.

It is understood that the representative methods of the present invention do not need to continue after initial registration and password transmission. Likewise, the process may me discontinued at some point in time by downloading a lifetime password which authorizes the software indefinitely. For example, this may be desirable after the software is deemed obsolete. It is further understood that the specific sequencing of events is not necessary for the proper implementation of the present invention. The invention further allows for compatibility with existing software or other security measures.

While the best modes for carrying out the invention have been described in detail, those familiar with the art to which this invention relates will recognize various alternative methods for carrying out the invention as described by the following claims.

What is claimed is:

1. A method for securing software to reduce unauthorized use of the software, the method comprising:

associating a series of passwords with the software for each authorized user prior to distribution of the software,

requiring entry of a first password upon first use of the software; and

subsequently requiring entry of another password to continue using the software.

2. The method of claim **1** wherein the authorized user is a group having a separate copy of the software for each of at least two end users.

3. The method of claim **1** further comprising including not more than one of the passwords with the software for distribution to each authorized user.

4. The method of claim 1 further comprising obtaining at least one password from an authorized representative of the software.

5. The method of claim 4 wherein the step of obtaining comprises electronically communicating with the authorized representative.

6. The method of claim 1 further comprising:

requiring communication of registration information associated with the end user to an authorized representative of the software prior to communicating the password to the software.

7. A method of securing software comprising:

disabling operation of the software until a password in obtained;

enabling operation of the software for a predetermined interval after the password is obtained; and

repeatedly requiring a new password for continued operation of the software beyond expiration of the predetermined interval wherein the new password is determined using a previous password.

8. A method for securing software to reduce unauthorized use of the software, the method comprising:

requiring entry of a first password upon first use of the software;

subsequently requiring entry of another password to continue using the software; and

repeating the step of subsequently requiring entry of another password at scheduled intervals for continued operation of the software.

9. A method for securing software to reduce unauthorized use of the software, the method comprising:

requiring entry of a first password upon first use of the software;

subsequently requiring entry of another password to continue using the software; and

repeating the step of subsequently requiring entry of another password at regular intervals.

10. A method of securing software to reduce unauthorized use, the method comprising:

associating a series of passwords with the software;

requiring an end user to contact a representative to obtain a password previously associated with the software;

communicating a password previously associated with the software to the software, wherein the software is not functional until the password has been communicated; and

subsequently requiring a new password, the new password being obtained from the series of passwords previously associated with the software.

11. The method of claim 10 wherein the step of communicating comprises electronically communicating the password.

12. The method claim 10 wherein the step of communicating is performed automatically by the software and the authorized representative.

13. The method of claim 10 further comprising:

obtaining registration information associated with the end user as a precondition for performing the step of communicating the password.

14. The method of claim 13 wherein the step of obtaining registration information is performed substantially simultaneously with the step of communicating the password.

15. The method of claim 13 wherein the step of obtaining registration information is performed substantially simultaneously with the step of communicating the password.

16. The method of claim 10 further comprising:

obtaining registration information associated with the end user; and

encoding the registration information so it is not readily discernible.

17. The method of claim 10 wherein the step of communicating comprises communicating the password to the end user enabling the end user to supply the password to the software.

18. The method of claim 10 wherein the step of associating a password comprises associating a series of passwords with the software.

19. The method of claim 10 wherein the step of requiring a new password is performed at regular intervals.

20. The method of claim 10 wherein the step of requiring a new password is performed at intervals based on elapsed execution time of the software.

21. The method of claim 10 wherein the step of requiring a new password is performed at intervals based on elapsed time.

22. The method of claim 10 wherein the step of requiring a new password is performed at predetermined intervals.

23. A method of securing software to reduce unauthorized use, the method comprising:

requiring an end user to contact a representative to obtain a password previously associated with the software;

communicating a password previously associated with the software to the software, wherein the software is not functional until the password has been communicated;

periodically requiring registration information associated with the end user to obtain a new password, the new password being required for continued operation of the software.

24. A method of securing software to reduce unauthorized use, the method comprising:

requiring a password for the software to become operational;

repeatedly requiring registration information associated with the end user to obtain a new password, the new password being required for continued operation of the software; and

comparing the registration information with previously obtained registration information associated with the software to determine whether the end user is an authorized user.

25. A method comprising:

requiring an authorization code for software to become operational;

repeatedly requiring registration information to obtain a new authorization code for continued operation of the software;

comparing the registration information with previously obtained registration information; and

providing a new authorization code only if at least a portion of the registration information matches previously obtained registration information.

26. A method comprising:

disabling software from being functional until a first authorization code is entered;

repeatedly requiring a new authorization code after expiration of each of a plurality of varying intervals for continued operation of the software, the new authorization code being obtained from the representative.

27. A method of securing software comprising:

associating a plurality of passwords with the software, at lease one password being generated prior to the distribution of the software;

enabling operation of the software after a password has been entered;

periodically requiring a new password for continued operation of the software, the new password being obtained after providing registration information associated with a user;

comparing the registration information with previously obtained registration information;

providing a new password which allows continued operation of the software if the step of comparing indicates the end user is an authorized user; and

providing a new password which disables the software if the step of comparing indicates the end user is an unauthorized user.

28. A computer readable storage medium having data stored therein representing software executable by a computer, the software including instructions to reduce use of the software by unauthorized users, the storage medium comprising:

instructions for requiring an end user to obtain a password associated with the software;

instructions for disabling the software until the password has been communicated to the software; and

instructions for repeatedly requiring communication of a new password for continued operation of the software.

29. The computer readable storage medium of claim **28** further comprising:

instructions for obtaining registration information associated with the end user.

30. A computer readable storage medium having data stored therein representing software executable by a computer, the software including instructions to reduce use of the software by unauthorized users, the storage medium comprising:

instructions for requiring an end user to contact an authorized representative to obtain a password associated with the software;

instructions for disabling the software until the password has been communicated to the software; and

instructions for periodically requiring entry of a new password for continued operation of the software.

31. A computer readable storage medium having data stored therein representing software executable by a computer, the software including instructions to reduce use of the software by unauthorized users, the storage medium comprising:

instructions for requiring a password associated with the software;

instructions for enabling the software after the password has been communicated to the software; and

instructions for disabling the software after a predetermined password is communicated to the software.

32. A computer readable storage medium having data stored therein representing software executable by a computer, the software including instructions to reduce use of the software by unauthorized users, the storage medium comprising:

instructions for requiring a password associated with the software;

instructions for enabling the software after the password has been communicated to the software;

instructions for subsequently requiring a new password to be communicated to the software for continued operation of the software; and

instructions for automatically contacting an authorized representative of the software to communicate registration information and obtaining authorization for continued operation of the software.

33. A computer readable storage medium having data stored therein representing software executable by a computer, the software including instructions to reduce use of the software by unauthorized users, the storage medium comprising:

instructions for requiring an end user to contact an authorized representative to obtain a password associated with the software;

instructions for disabling the software until the password has been communicated to the software;

instructions for periodically requiring entry of a new password for continued operation of the software;

instructions for automatically contacting an authorized representative of the software to communicate registration information and obtaining authorization for continued operation of the software; and

instructions for encoding the registration information.

34. A method of securing software to reduce use of the software by unauthorized users, the method comprising:

associating a series of passwords with each unit of software;

requiring communication of registration information to an authorized representative for the software to receive a first password from the series of passwords associated with the software, the registration information being associated with an end user of the software;

periodically repeating the step of requiring communication of registration information to the authorized representative to obtain a subsequent password from the series of passwords for continued operation of the software, each password enabling operation of the software for a predetermined interval.

35. A method of securing software to reduce unauthorized use of the software, the method comprising requiring periodic communication of registration information associated with a user of the software to a remotely located password administrator to obtain a password which enables continued operation of the software wherein the password is determined based on a previously obtained password.

36. A method for reducing unauthorized use of software, the method comprising:

requiring an end user to contact an authorized representative of the software upon initial use of the software by the end user to obtain an authorization code;

communicating registration information associated with the end user to the authorized representative; and

providing an authorization code which disables the software if the registration information indicates that the end user is an unauthorized user.

37. A method for reducing unauthorized use of software, the method comprising:

requiring registration information to be entered during initial use of the software;

communicating the registration information to an authorized representative of the software;

determining whether the software has been previously registered;

if the software has been previously registered, determining whether the registration information matches at least a portion of the previous registration information;

communicating an authorization code to the software upon receiving the registration information if the software has not been previously registered or if the registration information matches at least a portion of the previous registration information, the authorization code allowing continued operation of the software for a first predetermined period;

after the first predetermined period has expired, requiring a subsequent authorization code for continued operation of the software, the subsequent authorization code being communicated only if registration information indicates the end user is an authorized user based on previously received registration information.

38. A method of securing software to reduce unauthorized use, the method comprising:

Associating a plurality of passwords with the software and distributing one of the plurality of passwords concurrently with the software;

repeatedly requiring an end user to contact a representative to obtain another one of the passwords previously associated with the software; and

communicating one of the passwords previously associated with the software to the software, wherein the software remains functional only until the password expires.

39. The method of claim **38** wherein the step of communicating comprises electronically communicating the password.

40. The method of claim **38** wherein the step of communicating is performed automatically by the software and the representative.

41. The method of claim **38** further comprising:

obtaining registration information associated with the end user as a precondition for performing the step of communicating the password.

42. A method of securing software to reduce unauthorized use, the method comprising:

associating a plurality of passwords with the software and distributing one of the plurality of passwords concurrently with the software;

requiring an end user to obtain another one of the passwords previously associated with the software;

communicating one of the passwords previously associated with the software to the software; and

periodically requiring a new password for continued operation of the software, the new password being obtaining from an authorized representative.

43. A method comprising:

requiring a password to enable operation of software for a predetermined interval;

disabling the software upon expiration of the predetermined interval;

periodically requiring a new password for continued operation of the software, the new password being obtained from an authorized representative after providing registration information associated with the end user;

comparing the registration information with previously obtained registration information;

providing a new password which allows continued operation of the software if the step of comparing indicates the end user is an authorized user; and

providing a new password which disables the software if the step of comparing indicates the end user is an unauthorized user.

44. A method of securing software to reduce unauthorized use, the method comprising:

associating a plurality of passwords with the software and distributing one of the passwords concurrently with the software;

repeatedly requiring an end user to contact a representative to obtain another one of the passwords previously associated with the software;

communicating one of the passwords previously associated with the software to the software, wherein the software remains functional only until the password expires;

obtaining registration information associated with the end user as a precondition for performing the step of communicating the password; and

modifying the password based on the registration information.

45. A method of securing software to reduce unauthorized use, the method comprising:

associating a plurality of passwords with the software and distributing one of the plurality of passwords concurrently with the software;

repeatedly requiring an end user to contact a representative to obtain another one of the passwords previously associated with the software, the password being determined using a previous password; and

communicating one of the passwords previously associated with the software to the software, wherein the software remains functional only until the password expires.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO : 6,044,471

DATED : March 28, 2000

INVENTOR(S) : DAVID S. COLVIN

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 9, Line 14, Claim 7: delete "in" and insert –is–.

Column 9, Line 55, Claim 12: After "method" insert –of–.

Column 9, Line 66, Claim 15: Delete "is performed ... the password" and insert –comprises obtaining registration information from a computer on which the software has been installed–.

Column 13, Line 49, Claim 42 Replace "obtaining" with –obtained–.

Signed and Sealed this

Thirteenth Day of March, 2001

Attest:

Attesting Officer

NICHOLAS P. GODICI

Acting Director of the United States Patent and Trademark Office